



Sailing the Cyber Sea

By JAMES G. STAVRIDIS *and* ELTON C. PARKER III

Secretary Panetta listens to brief on functions of combat direction center aboard USS *Enterprise*

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 2012		2. REPORT TYPE		3. DATES COVERED 00-00-2012 to 00-00-2012	
4. TITLE AND SUBTITLE Sailing the Cyber Sea				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) National Defense University, 260 Fifth Avenue, Building 64, Fort Lesley J. McNair, Washington, DC, 20319-5066				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 7	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

A career in the maritime profession brings a fair share of stormy and uncertain seas. To successfully navigate these seas requires constant studying, understanding, and operating by an internationally agreed-to set of standards and norms affectionately known as the Rules of the Road. There are “rules” like these that apply to all the “global commons”—what we in the Department of Defense have classified as domains, namely land, sea, air, and space—and accordingly, we are somewhat accustomed to existing and navigating within boundaries and respecting borders.

There is another domain that tests such classification and definition. It is similar to the seas in its sheer magnitude, seeming ubiquity, and lethal potential, but it is also unique in that it is not comprised of water and waves; rather, it consists of zeros and ones, optic fibers and photons, routers and browsers, satellites and servers. This is, of course, cyberspace, the new global commons, a medium

a few servers and hubs being connected to devices that had less computing speed and power than today’s digital watches; thus, it was relatively easy to regulate traffic. By the early 1990s, however, there were a million devices connected to the Web, and in 2011, we surpassed one billion devices connecting us around the globe. Never before has information-sharing been so easy and so potentially disrupting . . . and that’s just *today*.

Tomorrow’s evolution promises still more mobility on faster, smaller, and smarter devices. As this domain grows, morphs, and evolves, so does our dependence on it. We continue to find new ways to provide accessibility, creating new forms of human interaction that bring us ever closer together, at least virtually. Whether through email, instant messaging, chatting, tweeting, blogging, social networking, retail activity, or business interactions, military organizations, government entities, nongovernmental organizations, and private and public ventures every day sail the vast and untamed Cyber Sea.

between the Supreme Allied Commander Europe (SACEUR) Facebook postings and tweets, we have been able to form almost 13,000 connections, and U.S. European Command (USEUCOM) blog entries have been viewed more than 185,000 times over the last 2 years. But those numbers pale in comparison to the potential of connections that exist in this still vast and untamed realm. For instance, Facebook tops Google for weekly traffic in the United States; Lady Gaga and Justin Bieber have more Twitter followers than the entire populations of Zimbabwe, Cuba, Belgium, Greece, Portugal, or Sweden; there are over 200 million public blogs.

Furthermore, it took radio approximately 38 years to reach an audience of 50 million, television 13 years, the Internet 4 years, and the iPod 3 years, while Facebook added 200 million users in less than 1 year. And finally, if Facebook were a country, based on population it would be the third largest in the world behind only China and India.

With each of these potential connections, we forge one link in the chain of understanding—eventually galvanizing a foundation of trust vital to exchanging ideas, communicating, collaborating, and cooperating with one another. Still, although the utility of social networking is obvious, the initial difficulty of obtaining access to Facebook and other social networking sites on a government network can be discouraging and frustrating. We need to do better. We need to be more openly connected. The use of social media is a great idea that is growing in popularity and can be a great tool for all kinds of activities. Audience size can be very large and messages disseminated quickly. We need to friend on Facebook, to blog, and to tweet. We need rich site summary (RSS) feeds and podcasts, and we need to be LinkedIn. Those and many others are all important tools in making key and valuable strategic connections to increase the positive correlation among words, deeds, and consequences.

Another example of the potential advantages and benefits that the connectivity and expanse of the cyber realm provide can be found in perhaps one of the least likely places—Afghanistan. Within a decade or two, paper money will no longer exist, and electronic banking and other transactions

*the Cyber Sea is the ultimate expression of freedom,
as it cannot be constrained by national or international lines
drawn on any map or chart*

referred to herein as the Cyber Sea. Upon it, we set sail each day in the company of a billion other adventurers—many embarking on voyages with distinctly crossed purposes. Together, we power up our netbooks and tablets, grab our smartphones, and use a vast array of ports (and portals) to connect to the rest of the world at *the speed of thought* in all sorts of different vessels, vehicles, and crafts.

Unlimited Potential

The Cyber Sea is the ultimate expression of freedom, as it cannot be constrained by national or international lines drawn on any map or chart, and is only seldom impacted by any sort of boundaries. As with the frontier days in each new domain, the potential for good is limitless; but because the realities of human expansion, commerce, and interaction typically outpace policies and regulations, much as during the days of the Wild West and early sea-faring expeditions, outlaw behavior is rife, and the *potential* for piracy, attacks, and conflict forever looms just over the horizon. To highlight this, recall the infancy of the Internet when it was comprised of only

In the military realm, when we speak about the cyber domain, it is easy and tempting to frame the discussion only in terms of cyber warfare or cyber attack. Although those are important dimensions of the subject, the topic is much broader, so the discussion on the matter must be much broader as well. We live in an increasingly interconnected world, a competitive marketplace where the primary commodity traded is ideas, a 24/7 news cycle with near-instant reporting and widespread dissemination of stories. It is a teeming, tumultuous, and exhausting marketplace, and all of us must continue to compete for our market “share.” In this world, information is power—and that power is magnified exponentially when *shared*.

We must embrace traditional forms of sharing (press interviews, newspapers, print magazines, and so forth) and then combine them with newer forms like blogging, tweeting, and posting on Facebook. As an example,

Admiral James G. Stavridis, USN, is Commander, U.S. European Command, and North Atlantic Treaty Organization Supreme Allied Commander Europe. Commander Elton C. Parker III, USN, is Military Assistant to the Vice President for Academic Affairs at the National Defense University.



David Shankbone

Occupy Wall Street protesters use Internet to organize and communicate from Zuccotti Park in New York City, September 2011

will take its place. This will further connect us in ways that we have not yet begun to assimilate into our societies and our cultural norms—particularly in the United States. As the saying goes, follow the money. As it continues to rebuild, Afghanistan may skip brick and mortar banking, shifting from paper money and going directly to cell phone transactions and electronic deposits. The vast majority of the Afghan National Security Forces are currently being paid electronically and, after biometric vetting, can access their money through cell phones. This reduces the opportunity for corruption, taking out layers of distributed paper money and the associated temptation to skim large amounts at each layer. Such a process allows the Afghans to use the electronic medium around their entire country.

Storm Clouds on the Horizon

Of course, while the new mechanisms and technologies provide means of connecting and empowering the next generation, they also enable voices and provide conduits for the spreading of nefarious ideologies,

for proselytizing, and for engaging in illicit activities in this largely unregulated virtual domain. As we keep a weather eye on the horizon of the Cyber Sea, we need to look at the underlying technologies and their transformational effect on our culture, our institutions, and our social fabric. We must

another example of the advantages of the cyber realm can be found in perhaps one of the least likely places—Afghanistan

also ascertain how all those things connect and interact to detract from or enhance our collective security. Each tidal wave brings potential challenges to that security that we ignore at our peril—cyber events can run the gamut from low-level observation to denial-of-service attacks to destruction of infrastructure; from espionage and intrusion to actual kinetic effects; and from crime to war.

On any given day, we may fall prey to hackers, identity thieves, and “hacktivists.” Our systems are bombarded by botnets and viruses. Trojan horses, worms, spyware, and spam all exist. We know these threats are real. According to the professionals at U.S. Cyber Command who are tasked with leading the Department of Defense’s (DOD’s) effort in the cyber domain, on an average day, DOD networks are probed approximately 250,000 times an hour; there are foreign intelligence organizations attempting to hack into U.S. computers; and terrorists are active on more than 4,000 Web sites. In 2010, a DOD contractor’s cyber defenses were breached and more than 24,000 files and pieces of data were stolen.

These seas are stormy indeed and they are just as unforgiving on individual humans cast adrift as they are on business enterprises and even nation-states. Here in Europe, this issue has particular resonance. In April 2007, the three Baltic republics of Estonia, Latvia, and Lithuania each had a series of denial-of-service attacks predominantly focused on Estonia and its financial systems. The

following year, the Republic of Georgia experienced not only a cyber attack, but a nearly simultaneous physical attack as well. The attacks themselves were challenging, though not insurmountable. What was more difficult was attributing the attacks and determining their origin. While bombs and missiles tend to leave “fingerprints” and come with a return address, photons on fibers are tough to track. As former Deputy Secretary of Defense William Lynn has stated, “A keystroke travels twice around the world in 300 milliseconds, but the forensics necessary to identify the attacker may take months.” Thus, despite not being able to precisely determine the origin of the cyber attack for attribution, this situation still showed the disastrous effects that can be achieved when combining the two forms of offensive warfare, solidifying the reality of cyberspace as a legitimate warfighting milieu.

This attribution and prosecution effort is further hampered by the fact that there is really no agreed-upon definition of what constitutes a cyber attack, nor is there a physical result of the attack in most instances—no crater, sunken ship, or blown-up safe. While the target is usually data, the effects can range from exploitation to degradation to destruction, and because data may not seem as tangible as some other more traditional types of targets, the effects may not appear as dramatic. The long-term effects, however, may actually be more devastating and costly, both in economic and human capital. Thus, to the victim, an attack is an attack, regardless of whether the weapon is a bomb or a botnet. Avatars and icons help to perpetuate a sterile and inorganic environment that tends to create a false sense of security and detachment, but injury, destruction, and death can be caused with comparable ease in this age of “dot combat.”

A particular example of this is the increasingly rapid and far-reaching terrorist use of cyberspace. Over the last 10 years, for instance, the number of Web sites devoted to what we in the West consider Jihadist terrorist sites has increased a thousand-fold, exploiting the freedom of the Web as a forum to spread poisonous propaganda, raise funds, and recruit converts. Jihadists also use the Internet as a virtual classroom to teach how to make bombs and plan attacks, ultimately even coordinating and carrying out attacks online. In a sense, for terrorists, the Internet has become a low-cost worldwide command and control network with unlimited nodes and zero main-

tenance requirements or overhead expenses. They are adept at adopting off-the-shelf tools to more fully exploit the lack of boundaries, policies, and regulations, as well as the anonymity found within this domain. Make no mistake—our enemies are as smart as they are well-funded, and thus innovation is definitely a two-way street.

*finding the balance
between empowering the
disenfranchised without
enabling the iniquitous can
and will be arduous and
daunting*

Balancing Open Access and Security

All this leads to an important question: how do we—individually and collectively—balance free and open access to such a virtual realm with the protections and regulations necessary to ensure our continued access to an environment that is safe and secure and contributes to the prosperity of humanity as a whole? The same technologies used by ordinary people to connect, inform, and educate are also being used by those who wish to harm, traffic, and degrade. There is a tension between that desire for openness and the very legitimate concern to protect our networks and our citizens. Whether mitigating the threat of industrial espionage, ensuring system redundancies in our Internet-dependent infrastructure, or improving cyber-forensic techniques to conduct investigations and precisely attribute the source of a cyber attack, *those with a stake in cyber security are in pursuit of the same goals: maximum protection of proprietary information while enabling seamless connectivity, functionality, and redundancy.*

Finding the right balance, the right setting on the rheostat, is key. If we want to compete in the current marketplace of ideas, if we want to fully take advantage of advances such as telemedicine, biometrics, terrain mapping, virtual collaboration, and the incredible array of user developed and user friendly applications, we need to get this correct. We need to secure our cyber networks to our advantage, not our detriment. Within the U.S. Armed Forces today, we wrestle with this dichotomy—even at the highest levels. To echo the former Vice Chairman of the Joint Chiefs of Staff, General James

Cartwright, “we cannot allow the chain of command to break the chain of information.” To ensure the continued flow of information, traditional stovepipes (which some may refer to as *cylinders of excellence*) that impede the cross-flow of ideas must be broken down. We need to develop meaningful policies, design and build innovative technologies, and otherwise inform the debate in order to bridge the “needs-technology-policy” gaps.

We have seen the positive *potential* of this medium in action—whether it is in the jungles of Colombia, the streets of Tehran, or Tahir square in downtown Cairo—and most recently in Libya and Syria. In each case, activists and tech-savvy sympathizers joined forces, leveraging the connectivity and potential of the cyber domain with the result being, as Eric Schmidt and Jared Cohen wonderfully labelled it, a situation where “the revolution will be podcast,” with “political ‘flash mobs’ . . . reporting, tweeting and writing a bill of human rights for the Internet Age.” As those who enjoy freedom of speech, press, religion, assembly, and political self-determination can attest, finding the balance between empowering the disenfranchised without enabling the iniquitous can and will be arduous and daunting, and the sheer number of users—one billion and growing—only exacerbates the challenge.

If we are going to successfully exist in this domain, we need to do so together, combining the military and civilian, foreign and domestic, and public and private sectors. Each nation has its own sovereignty, law enforcement, approach to privacy, systems and mores, and networks and technologies; however, in cyberspace, perhaps more than any other domain in which we are used to operating, the collective whole truly is greater than the sum of all of us working individually.

As with most endeavors, words matter—taxonomy is important. Thus, the first step is to agree on a set of definitions, formulate terms of reference, and establish a common lexicon. For the most part, this already exists in and throughout the military-technology world, but it has not truly translated or resonated to others outside this collective. Much as we continue to struggle to establish the physical boundaries of cyberspace, we need to determine what does and does not constitute a cyber attack. Criminal activity? Espionage? Cyber war? Hostile intent? We then need to determine and agree on what action is necessary and justified in each situation, based on



U.S. Air Force (Jeremy Burns)

Military members of several countries participate in multinational C⁴ operations during exercise Cyber Endeavor in Grafenwoehr, Germany

perhaps still-as-unwritten laws that govern action in this untamed sea during times of both war and peace. These are admittedly very militaristic terms; however, action in this domain will most often *not* be led by military personnel, so we *must* ensure our interagency community experts, as well as industry professionals, are involved with this discussion from the outset. And here at the North Atlantic Treaty Organization (NATO), they have been. As a result, in our vernacular, we have begun to establish what we call “rules of engagement,” rules that all 28 member nations understand and to which they agree.

NATO Cyber Actions

In mid-November 2010, the leaders of the 28 member states of NATO gathered in Lisbon for a summit. One of the primary products of this successful meeting was the new *NATO Strategic Concept*, and one of the key focus areas of this seminal document as the Alliance looks to the future was the cyber domain. The Lisbon Summit tasked the development of a revised NATO cyber defense policy by midsummer, as well as an accompanying action and implementation plan. In June 2011, the political decision-making body of NATO—the North Atlantic Council—adopted the new NATO Policy on

Cyber Defence, coupled with an Action Plan, fulfilling the tasking from Lisbon. Working with our Allies and taking lessons learned from events such as the 2007 cyber attacks on Estonia, NATO’s new policy focuses on improving a coordinated multinational approach and enhancing our collective and individual cyber defense capabilities to prevent threats and improve our responses.

In 2003, NATO founded the Cooperative Cyber Defence Centre of Excellence in the Estonian capital of Tallinn. It was accredited as a NATO Centre of Excellence in 2008. It is a multinational organization dealing with education, consultation, lessons learned, and research and development in the field of cyber security. The center’s mission is to enhance the capability, cooperation, and information-sharing among NATO nations and partners in cyber defense. Additionally, the center recently established an important and formal relationship with Symantec Corporation to promote cooperation on the research of online threats and counter-measures. The collaboration between the two organizations helps this center of excellence further explore new ideas to best understand, operate, and navigate within the still ungoverned and *undergoverned* spaces of this domain.

We have also established the NATO Computer Incident Response Capability (CIRC), which fulfills the summit mandate that NATO will enhance its ability and capacity to identify, assess, prevent, defend, and recover from a cyber attack. This center will be fully operational in 2012, and this is an important step in expanding a function to support cyber warning and damage assessments as part of a single integrated crisis management structure. Additionally, since it appears increasingly clear that cyber will play a role in any future crisis, we need to integrate cyber warning into our planning, and possibly develop ways to assess damage from a cyber attack as well as be able to determine how cyber attacks align with the employment of other instruments of power (diplomatic, military, economic, and others) in a crisis. Thus, we have established a Cyber Defence Cell as part of our new Crisis and Operations Management Centre, which will include the ability to enhance national and international cyber knowledge support into the shared system of warning, assessment, and crisis response.

If NATO itself is attacked, the CIRC will lead the technical defense and recovery responses, in conjunction with the Cyber Management Board, which has sole responsibility for coordinating cyber defense

throughout the Alliance via a series of memoranda of understanding between each nation's cyber defense organization and the board. If an individual Ally is attacked, however, things get a little more complicated, particularly when it comes to collective defense. Understanding all this within the context of the original Washington Treaty, signed during a very different time in this world in 1949, is paramount. Article 5 of the NATO treaty truly is the heart of the agreement—the bedrock that states an attack on one shall be considered an attack on all. Article 6 of the treaty goes on to define what constitutes an armed

of the team, and we are there in many ways to support the other interagency community members. Thus, we need to continue to try to understand cyber security in the larger interagency context, perhaps learning lessons from another comprehensive approach, one applied to the transnational and transagency challenge of illicit trafficking.

We have been able to forge and strengthen outstanding interagency and international bonds at the Joint Interagency Task Force–South in Key West, Florida, as well as a similar organization called the Joint Interagency Counter Trafficking Center here

in coordinating activities as well as creating the right incentives to participate. One way is highlighting the participation of such companies, producing a catalogue of trusted firms capable of offering security services and components. A primary condition for inclusion in such a list would be a commitment and contribution to the evolving information-sharing environment. And there are other ways.

NATO's cyber defense experts rely heavily on the partnerships formed across all of our Allies, both in the military and civilian realms. Increasingly, we are finding we need to develop and leverage the strong bonds with the private sector as industry will be absolutely essential as we move forward. This is also where the bulk of unrestricted innovative thinking resides. We recently convened a conference at NATO headquarters attended by corporations, academics, military members, and a wide variety of government officials from many nations to explore these public-private sector linkages, and how best to integrate them into a larger comprehensive approach in the cyber domain. Many wonderful conversations produced some outstanding initiatives that we will pursue energetically in the coming weeks and months. Such conferences will be regular occurrences as we start to lay the foundation for long-term collaboration and cooperation.

DOD has already begun to explore how industry can help in this regard through a public-private partnership called the Enduring Security Framework. Under this arrangement, the chief executive and chief technology officers of major information technology (IT) companies now meet recurrently with senior officials in both DOD and DHS, as well as with the Director of National Intelligence. Within NATO, we have started the conversations to examine creating a similar framework wherein key European agencies, businesses, and governments are selected to participate in sharing information on cyber security. This information collaboration would include everything from threat assessments to policy debates to research and development initiatives. That final category would provide a potentially large return on investment as we seek to match the defense industry's current excessive IT acquisition cycle (which ranges between 7 and 8 years) to the technological development cycle (which averages 1 to 2 years—just 24 months to develop the iPhone, for example). As Deputy Secretary Lynn put it, “In less time than

although it is an incredibly complicated thing to do, internationalizing cyber security is absolutely possible

attack, focusing on geography, attacks on territory, ships at sea, attacks on aircraft, troop formations, and the like. In 1949, however, few, if any, could have conceived of this new cyber world. As a result, within NATO in particular, we need to determine what defines an attack. Does it change from one member of the Alliance to another? Again, each nation has its own sovereignty, its own laws, its own law enforcement, and its own approach to privacy and security.

How Allies will respond to a cyber event of significant magnitude or the set of measures Allies will endorse in response to a cyber attack are decisions individual nations must make. However, NATO's new cyber policy makes clear that any decision on collective response (invoking Article 5) will be a political one made by the senior policymakers of the Alliance and member nations, and not by military or technical response teams. Of note, the only time NATO has invoked Article 5 was on September 12, 2001, following the 9/11 terrorist attacks on the United States.

Collaboration in the Larger Context

This new and undeniable aspect of warfare is likely to manifest itself more as the methodology of warfare continues to evolve. We need to understand this new cyber dimension of warfare and how to contend with it, and we need to come to grips with the notion that military involvement in this domain is but a small piece of the puzzle. In the United States, the Department of Homeland Security (DHS) is clearly and correctly the lead in this endeavor. DOD is merely one member

in Europe. These are potential models that could be applied to the world of cyber security, perhaps in the form of a joint interagency task force, ideally including international law enforcement agencies and other elements as the organization grows and develops.

Finally, though government has a large responsibility to provide mechanisms for securing our interests in cyberspace, cyber security is, as Sailors say, an “all hands on deck” evolution. Although there are at times strong crosscurrents between what we traditionally view as the role of the national entity and the role of public-private enterprises vis-à-vis our comprehensive security, we need to engage the experienced professionals in industry and in international organizations. Best practices are already shared among many cyber security experts in forums worldwide. However, a general lack of trust among the various players (to include corporations, government entities, and even nations themselves) precludes the accelerated growth of our cyber defense capabilities. We need to get past this suspicion and work together toward our common goals—it is clearly within our *shared* vital national interests.

If corporations are to invest real energy in sharing evolving cyber capability—be it in the form of human capital, investment capital, or actual hardware and software—we need to ensure the incentives are clear. What advantage is there for industry to participate? How will such collaboration and cooperation enhance their relative competitiveness and image and increase their bottom line? We have found that NATO can play a key role

it would take us to prepare and defend a budget, and then get Congressional approval for it, [Apple] gets an iPhone. It's not an acceptable trade."

New Thinking

In the context of security, unleashing the power of the Cyber Sea has changed everything—except our way of thinking. We simply cannot solve new problems using old thought processes. We need to continuously evolve. And we need to continue testing our theories and doctrine with joint, interagency, and international exercises and simulations. The Defense Advanced Research Projects Agency (DARPA) is creating a "mock Internet," a simulation training range where we can test security measures, responses to attacks, and how best to integrate the different capabilities and capacities each player brings to the table.

In 2010, DHS conducted Homeland Security Exercise Cyber Storm 3, a cyber incident response framework exercise. It included Federal and state entities, the private sector, and international organizations, all brought together to evaluate strengths and weaknesses of current policies, tactics, procedures, and capabilities. We need to continue conducting such hard-hitting evaluations and tests. Through them, we are learning we cannot afford to limit our own access to valuable information to protect ourselves from potentially harmful activity. Rather, we must be technically agile and politically courageous enough to get ahead of those who seek to do harm in cyber space. It is maneuver warfare on a cyber scale, and we must be swift.

In addition, in September 2011, U.S. European Command held an exercise called Combined Endeavor, a communication and computer network exercise where international military, industry, and academic professionals from 28 nations and organizations gathered to collaborate and improve partnerships with the end goal of strengthening collective cyber defense capabilities. The theme for this year's exercise was "Coalition Information Dominance," and the sessions focused on improving international cyber defense postures, operationalizing cyber information sharing, and institutionalizing coalition cyber training. Similarly, in December, NATO conducted its major annual cyber exercise, Cyber Coalition 2011. More than 100 specialists took part in the cyber defense exercise in NATO headquarters in Brussels and Mons, including national cyber defense facilities in their respec-

tive countries, all coming together to test technical and operational Alliance cyber defense capabilities. In both exercises, scenarios were designed that required action, coordination, and collaboration from technical experts, policymakers, and management bodies. Both were highly successful events and we learned a great deal. We learned that we face a shared challenge, and thus through open communication and collaboration, we will build trust between and among our nations. Most importantly, we underscored the fact that although it is an incredibly complicated thing to do, internationalizing cyber security is absolutely possible. It is also absolutely necessary.

This article began with an analogous reference to the Cyber Sea. As we engage the cyber world, it is interesting to contemplate the comparisons with the maritime domain, particularly within the context of the challenges mankind faced in bringing some order to the untamed oceans. It has taken humanity two or three thousand years to sort out how we operate on the sea; we have gradually created international maritime law, buoy systems, a global navigation grid, and charts to guide our way. In sum, we have built a system. And in the 1980s, the international community came together in the largest negotiating project in the history of mankind and created the United Nations Convention on the Law of the Sea. The treaty took a decade to negotiate. At more than 200 pages, it is an extremely complex canon; but with few exceptions, 195 different sovereign signatories guide their actions at sea by it.

Now, contemplate a similar undertaking regarding the Cyber Sea. We have been sailing upon that realm in earnest for about 20 years now, and really generating some waves for about the last 10. Yet for the most part, we still do not have reliable buoys, we still do not have an enforceable navigation grid, and we still set sail without up-to-date charts. We cannot even really say we have the basic norms of behavior save a few very specific punitive laws for the most egregious acts. More importantly, we do not have a millennium to figure it out. We are running out of time. Our Secretary of Defense recently commented "there is a strong likelihood that the next Pearl Harbor that we confront could very well be a cyber attack." With each passing millisecond, this expanding medium grows in vulnerability faster than it grows in utility, and our institutional regulations and policies fall farther behind.

We need to catch up and eventually get out in front of this bow wave. We need to agree to specific terms of reference like "attack" and "incident" and what constitutes each. We need to agree to policy prescriptions that dictate proportionality of response, pursuit of attackers across national boundaries, be they geographic or virtual network lines, and others. The 2011 White House and Pentagon strategies on cyber go a long way toward each of these aims, as does the new NATO cyber policy—but we must push these efforts further.

And we need to do this collaboratively: within and across governments and their agencies, within and between public and private enterprises, throughout academic institutions, and within our shared homes. Cyber security requires complex and coordinated responses that move at the speed of thought. Diversity of capabilities, capacities, and responses to any cyber challenge should be seen as a strength, not a weakness—but only if the actions and tools can be used synergistically. This can only happen when all the interested parties adopt a common vision for security built on the foundation of trust and confidence, and achieved through coordination, cooperation, and partnering. No one of us is as strong as all of us working together. **JFQ**